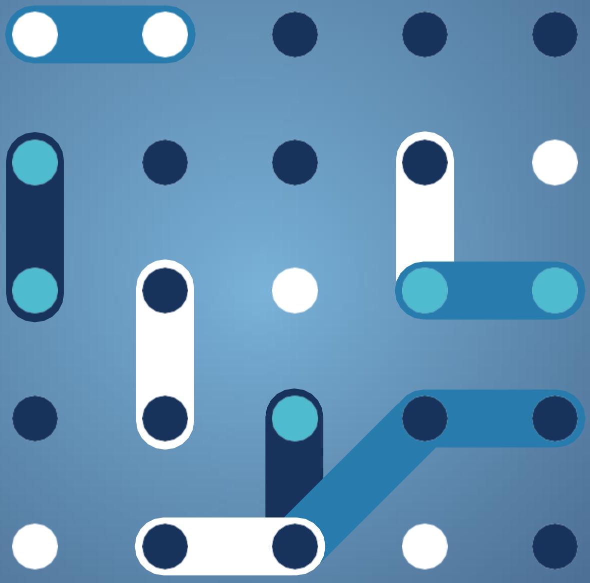
European Commission

bridge

Improving the cybersecurity and resilience of the Electrical Power and Energy System

Case study #6



June - 2023

AUTHORS

Clémentine Coujard, *Dowel Innovation*

Stéphanie Petit, *Dowel Innovation*

SUPPORT FROM THE BRIDGE SECRETARIAT

Martin Bracken, CLERENS, BRIDGE Secretariat

Niclette Kampata, ZABALA, BRIDGE Secretariat

Marcos Jareño, ZABALA, BRIDGE Secretariat

Agnieszka Gierej, ZABALA, BRIDGE Secretariat

ACKNOWLEDGEMENTS

The editors would like to acknowledge the valuable inputs received from the projects' coordinators and partners.

EUROPEAN COMMISSION

Directorate-General for Energy
Directorate B – Just Transition, Consumers, Energy Efficiency and Innovation Unit B5 – Innovation, Research, Digitalisation, Competitiveness

Contact: Felipe Castro Barrigon

E-mail: felipe.castro-barrigon@ec.europa.eu

European Commission

B-1049 Brussels

Improving the cybersecurity and resilience of the Electrical Power and Energy System

Case study #6

June 2023

Directorate General for Energy 2023

LEGAL NOTICE

This document has been prepared for the European Commission. However, it reflects the views only of the authors, and the European Commission is not liable for any consequence stemming from the reuse of this publication. More information on the European Union is available on the Internet (http://www.europa.eu).

CONTENTS

1 The digitalisation and interconnection of power systems raise new cybersecurity issues, with potential critical impacts on society

1.1 Context

Digital technologies are playing an increasing role in the transition of the electrical power and energy system (EPES) towards more sustainability: enhanced monitoring, forecasting and control contribute to increase energy efficiency and reduce consumption; facilitate the integration of higher shares of renewable electricity; and enable to activate new sources of flexibility in the system.

However, such technological advances come along with new risks in terms of cybersecurity: the growing use of digital devices and the increasing interconnection of systems trigger new vulnerabilities such as data breaches, worms, viruses, or hacker attacks. The multiplication of smart meters and IoT devices represent as many new access points within the electrical systems that are exposed to cyber threats. The electricity system needs to be prepared to tackle these threats, as some inherent challenges remain present, for instance legacy systems such as SCADA were not designed to include cyber protection requirements. Even more, the disconnection of an electricity network under cyber-attack can be complex and slow to implement, possibly leading to loss of services, blackouts, and cascading effects in other sectors of society.

To tackle such issues in the energy sector and other critical infrastructures, the European Union enforced some new legislation related to cyber protection. In 2019, the ''Cybersecurity Act'' introduced a framework for European Cybersecurity Certificates and reinforced the mandate of the EU Agency for Cybersecurity (ENISA). In early 2023, the NIS2 Directive was adopted, providing additional legal measures to boost the overall level of cybersecurity in the EU. The targeted entities shall, among other obligations:

- implement technical and organizational measures to prevent, detect and respond to incidents that could impact the security and continuity of energy supply. This includes data protection and privacy.
- report any incidents that could impact the security of that data, and share information amongst themselves such as cyber threats, attacked or adversarial tactics

1.2 Challenges

Implementing the NIS2 Directive, and more widely, ensuring the security and resilience of digitalised EPES implies to tackle some pending challenges:

- Share a common framework of data privacy and security principles, suited to the complex context of electricity grids (large scale, multiple layers, multiple interconnections), and also considering the human factor
- Dispose of reliable tools to evaluate the vulnerability of systems, detect and mitigate cyber threats that are in constant evolution, while considering/integrating the legacy equipment not designed to those purposes
- In case threats materialise, deploy resilience strategies that can limit the impact of the incidents on the electric system and its involved parties.

The next pages illustrate how a selection of BRIDGE projects contribute to tackling these issues.

2 Providing the necessary framework and tools to improve the cybersecurity and resilience of the digitalised EPES

This case study focuses on three main building blocks that are investigated by a selection of H2020 funded projects dealing with cyber security of power systems:

- **A cybersecurity culture and framework** to ensure data privacy as well as secured data exchanges in all operations and services
- **Tools to detect and mitigate cyber threats,** from the overall risk assessment to the detection and mitigation of anomalies and intrusions
- **Tools to improve the system's resilience to incidents,** and limit the impact of faults occurring on the electrical system.

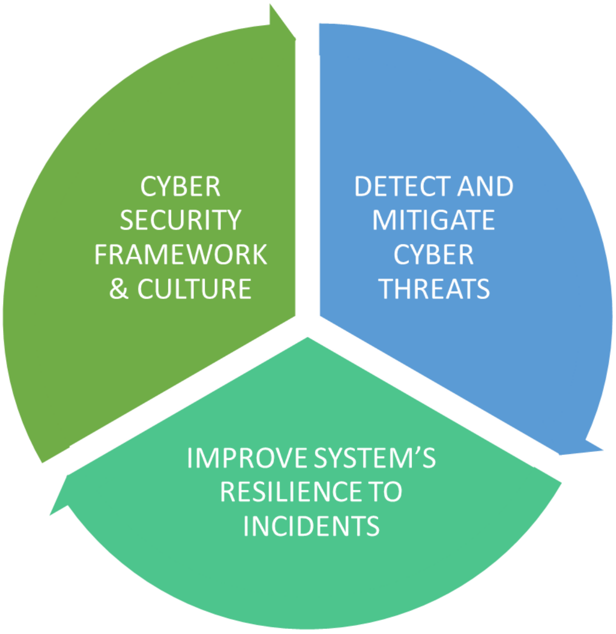

CYBER SECURITY FRAMEWORK & CULTURE
DETECT AND MITIGATE CYBER THREATS
IMPROVE SYSTEM'S RESILIENCE TO INCIDENTS

Figure 1 The three building blocks to improve the cybersecurity of digitalised EPES

The case study proposed focuses on three H2020 projects that address those buildings blocks complementarily:

PHOENIX

Sept 2019 – Sept 2022

PHOENIX aimed to offer a cyber-shield armour to European Electrical Power and Energy System (EPES) infrastructure enabling cooperative detection of large scale, cyber-human security and privacy incidents and attacks, guarantee the continuity of operations and minimize cascading effects in the infrastructure itself, the environment, the citizens and the end-users at reasonable cost.

ENERGY SHIELD

July 2019 – June 2022

EnergyShield aimed to capture the needs of Electrical Power and Energy System operators and adapt and combine the latest tools for vulnerability assessment, anomaly detection and security related behaviour analysis with the end goal of integrating them into a defensive toolkit.

SDN-μSense

May 2019 – Oct. 2022

SDN-microSENSE intended to provide a set of secure, privacy-enabled and resilient to cyberattacks tools, thus ensuring the normal operation of the EPES as well as the integrity and the confidentiality of communications. SDN stands for software-defined network.

3 A cybersecurity framework and culture

Improving the cybersecurity of the electricity power and energy system implies to deploy a technical framework and foster human behaviours that will ensure the privacy, confidentiality, and security of data exchanges. Such framework will then allow for more secured operation, trading services, and sharing of knowledge.

3.1 Secured frameworks enable to ensure the privacy, confidentiality, and legitimacy of data exchanges

- **PHOENIX** designed a **Privacy Protection Enforcement** (PPE) framework for managing sensitive and confidential data using **mutual auditability signatures and advanced consent**[1]. It is implemented through the PRIMULA (Privacy, Reputation and Mutual Auditability) toolbox that enables managing the consent among the different parties (data subjects, data controllers and data processors) via **smart contracts**.[2] PRIMULA also provides consent auditing functionalities and reputation mechanisms to **assess the party's reputation** based on global perception of its behaviour.
- **PHOENIX** developed a **Secure and Persistent Communication Layer**[3] **(SPC)** that supports security, privacy and survivability by design, ensuring data acquired/served are legitimate and secured. The SPC Layer offers security over the legacy protocols that are currently used in EPES infrastructures. It adopts a data-centric approach based on federated Distributed Ledger Technologies (DLT) to achieve a higher degree of persistency, traceability, availability, integrity, and interoperability in the context of data communications. It is combined with a **Universal Secure Gateway** (USG) to securely interconnect with existing EPES ICT systems, APIs and standards.
- **SDN-microSENSE** developed a **secured blockchain-based Energy Trading Framework**[4] using Hyperledger Fabric blockchain technology to achieve secure and sustainable energy transactions between the participants of a permissioned blockchain network. It ensures that **energy and financial transaction-related data are not exposed outside** the set of organizations participating in the network, while allowing them to interact through smart contracts. The framework also integrates **security monitoring and reporting** procedures, via a distributed system comprising agents installed on the devices of the participants (e.g. smart meters or remote terminal units): the agent ensures the uncompromised status of the device, and in case of any anomaly, the device owner cannot participate in any auctions. Agents can also be equipped with process-hiding mechanisms in order to inhibit any attacker from discovering and tampering with the agent itself.

3.2 The cybersecurity culture in organisations depends on the human factor that needs careful assessment

- **ENERGYSHIELD** developed a **Cyber Security Culture Framework** and tested the corresponding **Security Behaviour Analysis tool**. The cyber security culture framework aims to assess the current security readiness of an organisation 's workforce. Based on a combination of organisational and individual security factors, it examines the organisational security policies and procedures in conjunction with employees' individual characteristics, behaviour, attitude, and skills. Each security metric is assessed using a variety of evaluation.

[1] Reference: https://phoenix-h2020.eu/wp-content/uploads/PHOENIX_D4.2.pdf

[2] Smart contracts are programs stored on the blockchain that run when predetermined conditions are met, typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement or time loss.

[3] Reference: https://phoenix-h2020.eu/wp-content/uploads/PHOENIX_D2.3.pdf

[4] Reference: https://ieeexplore.ieee.org/document/9247893

techniques, such as surveys, tests, simulations, and serious games[5]. These elements are then implemented in the Security Behaviour Analysis tool, paying special attention to user friendliness and business effectiveness, while clearly differentiating among the three distinctive security roles implemented: administrator, manager and user.

3.3 Sharing knowledge on threats and incidents between stakeholders can be performed and automated in confidentiality

The NIS Directive requires mandatory reporting of cybersecurity incidents by the EPES operators:

- In order to facilitate incident information sharing, the **SDN-microSENSE** project developed an **incident anonymiser**, enabling to anonymise the incident information that could identify the owner of the incident. It uses the Differential privacy technology for anonymising the incidents. The team elaborated an **Anonymous Repository of Incidents (ARIEC),** intended to store and share information about the detected incidents with other EPES. ARIEC ensures confidentiality, integrity and interoperability between data exchange parties. ARIEC can receive security incidents information from different sources: by automatic communication through the XL-EPDS or the S-RAF, and also, by direct reporting by a human operator (e.g., DSO Operator, Security Administrator or Power Plant Operator).
- On the same principle, **PHOENIX** developed the **Incidents Information Sharing Platform I2SP**[6], that allows different stakeholders to coordinate and share knowledge on cyberthreats. It enables to collect and share incidents' information and trained machine learning models **without the need to share sensitive information** across EPES operators and CERTs. It is designed as a pan-European platform for secure threat information sharing, that leverages Trusted Automated Exchange of CTI (Cyber Threat Intelligence) Information via Structured Threat Information Expression (STIX) format and private blockchain technology to **automate the threat sharing procedure** while offering privacy, data integrity, and interoperability. The extensive evaluation of the solution implementation indicated its capability to offer secure communication between participants without sacrificing data privacy and overall performance as opposed to existing solutions.

3.4 New methods and procedures will contribute to achieve the EC Directive's objective on certification framework

To accelerate the testing and certification of new EPES secure products in the market, the **PHOENIX** team established a series of **certification methods and procedures** through a newly created Cybersecurity Certification Centre based in the Netherlands. They serve as a European wide blueprint for cybersecurity, privacy and interoperability certification and provide organisation and process certification for product development, integration and manufacturing organisations.

[5] Reference: https://doi.org/10.3390/s21093267
[6] Reference: https://doi.org/10.3390/info13100463

4 Tools to detect and mitigate cyber threats

Cyber threats are constantly evolving: the solutions to detect and mitigate them shall consider this uncertainty factor and be capable to adapt continuously to new threats. Scenario simulations and self-learning techniques are therefore beneficial assets to serve such purposes.

4.1 Threat scenarios and simulations enable to assess vulnerability to cybersecurity risks

- **PHOENIX developed a methodology on threat detection, risk assessment and mitigation[7].** Guidelines for the design of unknown threat identification systems were proposed. EPES' cyber threats were identified, analysed and modelled, deriving threat scenarios and attack trees related to the 5 PHOENIX large scale pilots. The work also included the categorization of assets and systems into secure tiers, assisted by a risk assessment methodology and a software tool automating the calculation of the combined risk rate per PHOENIX large scale pilots.
- **EnergyShield** improved and tested a **Vulnerability Assessment (VA) tool[8]** that simulates attacker's behaviour within networks. It enables to create a digital twin or offline clone of the environment in order to simulate cyber-attacks. The tool assesses the attacker's most likely path and plots the probability of the attacker to reach and compromise the critical assets.
- **SDN-microSENSE developed a Security and Risk Assessment framework (S-RAF)** intended to establish the necessary risk priorities and security policies, identifying possible threats and vulnerabilities and determining the corresponding risk levels for each entity of EPES. S-RAF assesses the level of risk in all the involved EPES devices and systems by analysing a) current smart & IoT devices, b) legacy SCADA & ICS devices, c) smart meters d) other software/hardware devices connected to EPES network and e) all the energy-related personnel and stakeholders (energy operators, consumers, prosumers, utilities, etc). A cumulative risk is calculated to perceive the security state at the level of mission-critical assets that belong either in the same business workflow, or in the same physical (or virtual) networks.

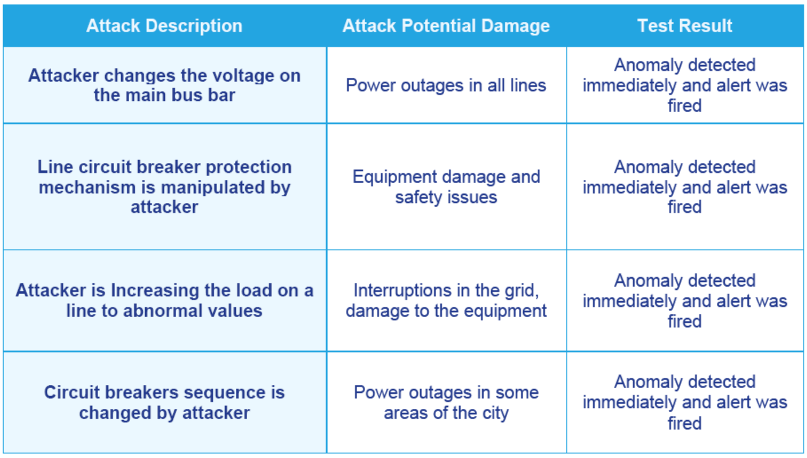
4.2 Artificial Intelligence enables new approaches to threat detection and mitigation

- **PHOENIX developed some AI-based services supporting Situation Awareness, Perception and Comprehension** and **Incidents Mitigation and Enforcement Countermeasures**. These include privacy-preserving federated learning techniques for uncovering anomalies, co-simulator approaches and their integration into a decision support system, conducted over data gathered at the project's trial sites, as well as optimal calculation of Mitigation Strategies to assist the risk management of the EPES. **These services were tested with a scenario of cyber-attacks on 5G networks**: the detection and mitigation measures were applied to a hydroelectric power plant (HPP), where cyber-attacks were performed in a 5G-enabled smart meter that measures power production and transmits measurements to PPC's control center through the use of 5G network function virtualization (NFV) technologies. The measures were used to detect the attacks and perform necessary mitigation actions for restoring the HPP operation.

[7] Reference: https://phoenix-h2020.eu/the-phoenix-project-achievements-summary/

[8] Reference: https://energy-shield.eu/wp-content/uploads/2022/06/EnergyShield-Whitepaper_VA_FOR_v1.1.pdf

- **EnergyShield** adapted and improved an **Anomaly detection (AD) tool**[9] that analyses the networks and points out **unexpected events**. It is a software and hardware tool that uses Machine Learning to enable the real-time detection of anomalies covering the monitoring part. The tool was deployed at two pilot sites: in Italy on an HV/MV substation, to monitor the operation of 5 different lines (circuit breaker and current measurement) and main bus bar (voltage measurements); and in Bulgary on a hydro power plant to monitor its operational parameters (temperature, power, flow, and pressure sensors). After learning the normal behaviour of the sub-station/power plant process, the tool detected anomalies in real-time. The next table (presented as a result at the end of the project) gives an overview of the attacks simulated and results obtained.



Attack Description	Attack Potential Damage	Test Result
Attacker changes the voltage on the main bus bar	Power outages in all lines	Anomaly detected immediately and alert was fired
Line circuit breaker protection mechanism is manipulated by attacker	Equipment damage and safety issues	Anomaly detected immediately and alert was fired
Attacker is Increasing the load on a line to abnormal values	Interruptions in the grid, damage to the equipment	Anomaly detected immediately and alert was fired
Circuit breakers sequence is changed by attacker	Power outages in some areas of the city	Anomaly detected immediately and alert was fired

Figure 2: Overview of attack types10

- **In EnergyShield,** the **distributed denial-of-service (DDoS) mitigation module** defends the systems against incoming traffic flooding. The module leverages machine learning-based algorithms to detect and mitigate DDoS attacks on the communication infrastructure. During the testing phase the tool successfully proved to block or mitigate the DDoS attacks, through **immediate dynamic response**. This was achieved via a novel approach combining epidemiological analytics and dynamic modelling methods[11].
- In **EnergyShield**, SIEM functionalities were adapted, details about the deployment within the EnergyShield Toolkit were added, while agents were installed to monitor onsite endpoints to give an overview of what is happening in the organisation. It provides an open source host-based **security monitoring service**, that can be easily integrated with other tools and analytical services to extend its efficiency and scope.
- **SDN-microSENSE** developed a Cross-Layer **Intrusion Prevention and Detection System** (XL-EPDS) to protect the EPES from cyber threats on the key communication protocols used by SCADA, i.e. DNP3, Modbus and IEC-104. The tool integrates, among others:
    - A Security Information and Event Management (SIEM) function, intended to continuously monitor, control and correlate the operations performed at Control Centres, TSOs, DSOs and Smart Meters. The SIEM platform is composed of distributed agents responsible for the event collection, normalization and transfer of data; an engine to filter, aggregate, and correlate the events collected by the agents, and to generate alarms; a database for data storage; and a dashboard for data visualization.
    - The Intrusion Detection and Prevention System function, that provides appropriate specifications regarding the normal operation and utilisation of industrial protocols (such as Modbus, DNP3 and IEC 60870-5-104).

[9] Reference: https://energy-shield.eu/wp-content/uploads/2022/06/EnergyShield-Whitepaper_AD_SIGA_1.0.pdf
[10] Reference: https://energy-shield.eu/wp-content/uploads/2023/02/EnergyShield_D6.3-Field-trial-evalution_V2.0.pdf
[11] Reference: https://energy-shield.eu/wp-content/uploads/2022/06/EnergyShield-Whitepaper_DDoSM_L7D_v1.1.pdf

- The Anomaly Detection function, using Machine Learning (ML). A number of ML-based detectors were developed, each one focusing on the detection of incidents associated to an individual SCADA protocol.

5 Tools to improve the system's resilience to incidents

In case the preventive cyber protection schemes cannot fully block cyber-attacks, then some curative tools shall take over to limit their impact on the power system and its associated services. Artificial Intelligence allows for new solutions to improve the system's resilience to incidents.

SDN-microSENSE developed an Optimization Tool for Self-healing and Clustering tool providing a self-healing method to the power system to minimize the unsupplied loads and increase the electric grid resilience during an incident in the infrastructure. Once an incident occurs the tool provides a safe electric topology by creating islands isolating the incident. Once the islanding scheme is deployed, the tool provides the necessary orders to maintain the energy balance in the islands acting as a tertiary control. Its specificities are detailed below.

5.1 AI-based techniques enable to propose intentional islanding schemes to isolate the fault and preserve the system…

- **SDN-microSENSE Islanding and optImisation fraMework**[12] (IIM) aims to support the operator in defining and applying an intentional islanding mechanism when a fault occurs on the electric system. The tool creates a new electric scheme with islands to divide the grid into different sectors, with the aim to isolate the elements that can cause problems in the grid and at the same time maintain the power supply to the maximum number of consumers. The tool uses Binary Genetic Algorithm to determine the islands. The maximum number of islands to be created is set as an input. However, the tool determines the number of islands to be created based on the connection strength of the nodes in the given configuration. This islanding framework was tested for two grid topologies, the CIGRE 15 benchmark model and the IEEE 30 test feeder, both modified to contain additional distributed generation.

5.2 … and to ensure the continuity of grid operation after such islanding

- **SDN-microSENSE REstoration Machine-learning framework** includes two complementary applications intended to operate automatically on the grid to improve its reliability. The first application, the Multi Agent system (MAS) provides the functionality to determine the black-start sequence on the system and the functionality to maintain the voltage and frequency during operation. The second tool maintains the energy balance in the islands created by the IIM (see previous section).
- The above-mentioned Multi Agent System (MAS) is focused on providing 1) Voltage & Frequency restoration and 2) Black Start optimal sequence re-connection of Distributed Energy Resources and loads. The tool can operate on either semi-centralised or distributed control modes. It was evaluated in a simulated low-voltage Microgrid developed in MATLAB/Simulink and results indicated that the proposed process ensured a distributed, fast, low throughput footprint and topology-invariant decision-making. Using empirical synthetic topologies, the scalability of the black start process was also demonstrated.

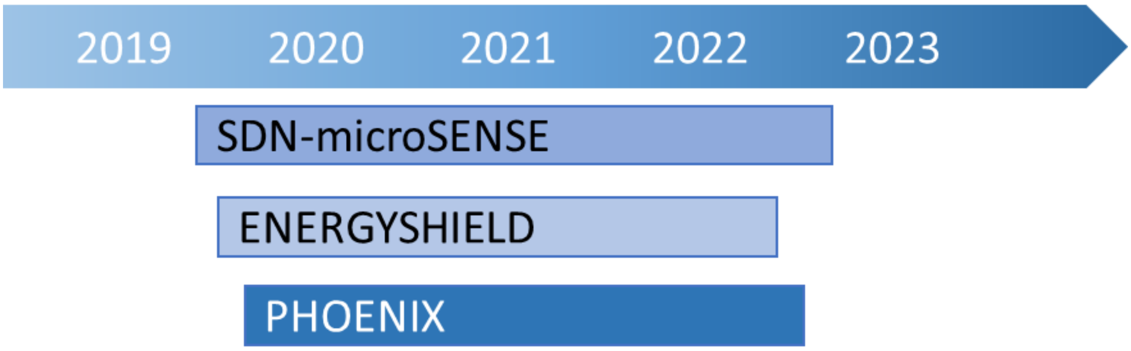
[12] Reference : https://ieeexplore.ieee.org/document/9247893

6 KEY TAKE AWAYS: facts & figures

Section 3: Providing the necessary framework and tools to improve the cybersecurity and resilience of the digitalised EPES
• Projects developed some privacy frameworks enabling the secured exchange of data, including mutual auditability, signature and consent mechanisms, data tracking and smart contracts. This allows to ensure secured internal operations, secured interconnections with other EPES, secured trading services, and the confidential sharing of incident information between different operators.
• The human factor is critical when deploying a cybersecurity framework: user-friendly tools have been developed to assess the security readiness of organisations based on the analysis of employees' behaviours.
• A new cybersecurity certification center was created to apply certification methods and procedures for product development, integration, and manufacturing organisations.
Section 4: Tools to detect and mitigate cyber threats
• The projects developed several tools to simulate cyber threats, assess the vulnerability of systems, and perform overall cyber risk assessment
• Using AI-based learning techniques, new tools were developed and successfully tested to assess normal operation parameters, detect anomalies, and propose mitigation solutions
Section 5: Tools to improve the system's resilience to incidents
• In case preventive actions are not sufficient to block the cyber-attacks, tools are required to ensure curative actions and limit the impact of incidents on the electricity system. The tools developed provide intentional islanding schemes to isolate the fault and avoid cascading effects, ensure electricity balance in the system further to such islanding, and determine the black start sequence if needed.

7 References

Timeline of the projects studied:



Projects information

Bridge project	Call	Goal	Website	Coordinator / Contact
PHOENIX 832989: Electrical Power System's Shield against complex incidents and extensive cyber and privacy attacks	Digital Security (H2020-SU-DS-2018-2019-2020) TOPIC: SU-DS04-2018-2020 Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches	Cyber-shield armour to European EPES infrastructure enabling cooperative detection of large scale, cyber-human security and privacy incidents and attacks, guarantee the continuity of operations and minimize cascading effects in the infrastructure itself, the environment, the citizens and the end-users at reasonable cost	https://phoenix-h2020.eu/	Capgemini Technology Services, France.
EnergyShield 832907: Integrated Cybersecurity Solution for the Vulnerability Assessment, Monitoring and Protection of Critical Energy Infrastructures		Develop an integrated toolkit that combines the latest technologies for vulnerability assessment, monitoring and protection, as well as learning and sharing. It will be tailored to meet the needs of EPES operators	https://energy-shield.eu/	Software Imagination & Vision SRL, Romania.
SDN-microSENSE 833955: SDN - microgrid reSilient Electrical eNergy SystEm,		Provide secure, privacy-enabled and resistant-to-cyberattacks tools to ensure EPES operation and the integrity and confidentiality of communications.	https://www.sdnmicrosense.eu/	Ayesa Advanced Technologies SA.

Credits: This brochure is financed by the European Commission and developed by DOWEL Innovation.

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

– by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

– at the following standard number: +32 22999696, or

– by email via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications from: https://op.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

Open data from the EU

The EU Open Data Portal (http://data.europa.eu/euodp/en) provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and non-commercial purposes.

Publications Office
of the European Union